Web Images Videos Maps News Shopping Gmail more ▾ Sign in

Google scholar signcryption IBE signature commitment private Search Advanced Scholar Search

Scholar Articles and patents ▾ 1900 - 2003 include citations ▾ Create email alert Results **1** - **24** of **24**. (**0.10** sec)

On the security of joint **signature** and encryption [PDF] from psu.edu
J An, Y Dodis... - Advances in Cryptology---EUROCRYPT 2002, 2002 - Springer
... VerDec(u) = VerDec(u). Thus, CCA2 attack wrt R disal- lows A to de-**signcrypt** any u **... Signcryption** only allows the receiver to be convinced that m was sent by S, but does not **...** We believe that non-repudiation should not be part of the definition of **sign- cryption** security, but we will **...**
Cited by 336 - Related articles - BL Direct - All 13 versions

Multipurpose identity-based **signcryption** [PDF] from psu.edu
X Boyen - Advances in Cryptology-CRYPTO 2003, 2003 - Springer
... purpose optimized IBSE scheme is as compact as most existing single-purpose **IBE** and IBS **...** instead of the usual notion of ciphertext unforgeability as studied in the **signcryption** model of [1 **...** also that ciphertext unlinkability only makes sense in a two-layer **sign- cryption** model like **...**
Cited by 223 - Related articles - All 31 versions

Compact and unforgeable **key** establishment over an ATM network [PDF] from psu.edu
Y Zheng... - ... 98. Seventeenth Annual Joint Conference of ..., 1998 - ieeexplore.ieee.org
... The example **signcrypt**,ion scheme is called SCSl and it uses a shortened version of the **...** described in Tables 3 and 4 are essentially message transport ,schemes using **sign- cryption**, security of **key** materials are guarant,eed by the security of the **signcryption** scheme against **...**
Cited by 27 - Related articles - BL Direct - All 12 versions

Distributed **signcryption**
Y Mu... - Progress in Cryptology---INDOCRYPT 2000, 2000 - Springer
... that Alice belonging to group Ga wishes to send a signcrypted message m to the group Gb and that Bob is one of recipients **...** In order to **signcrypt** the message, Alice needs to do the following **...** Computes r = Hk2 (m) and sj = k(xj a − ruj) mod q (j = 1, ..., n). – The **signcryption** is then **...**
Cited by 38 - Related articles - BL Direct - All 6 versions

Encrypted message authentication by firewalls [PDF] from psu.edu
C Gamage, J Leiwo... - Public Key Cryptography, 1999 - Springer
... Operation **Signcryption** Modified **Signcryption** DSA sign + ElGamal encrypt **Signcrypt** 1 EXP 2 EXP 1 + 2 EXP **...** 2. The challenge is simply a one-way hash of the message being signed and the witness value. **...** 4.3 Properties of Modified **Signcryption** Scheme **...**
Cited by 55 - Related articles - BL Direct - All 13 versions

Parallel authentication and public-**key** encryption [PDF] from ens.fr
J Pieprzyk... - Information Security and Privacy, 2003 - Springer
... to the random oracles, and q1 and q2 queries to the **signcryption** and de-**signcryption** oracles, respectively. **...** Advind−ada **SignCrypt**(A) = 2 Pr[d = b] − 1 = 2Pr[d = b (AskG AskR)]+2 Pr[d = b **...** necessarily appears in the queries asked to g. For each query asked to g, one runs the **...**
Cited by 19 - Related articles - BL Direct - All 11 versions

[PDF] Parallel **Signcryption** with OAEP, PSS-R, and other Feistel Paddings [PDF] from psu.edu
Y Dodis, MJ Freedman... - 2003 - Citeseer
... Moreover, using the scheme of [27], one can only **signcrypt** messages of length significantly less than k/2, while PbPS with an appropriate two-padding scheme allows a user to **signcrypt** messages of length close to 2k. **...** Table 1: A comparison of **signcryption** schemes. **...**
Cited by 2 - Related articles - View as HTML - All 6 versions

Efficient distributed **signcryption** scheme as group **signcryption**
DJ Kwak... - Applied Cryptography and Network Security, 2003 - Springer
... Thereafter, Mu and Varadharajan proposed the distributed **sign- cryption** using distributed encryption [MN99] in [MV00], where any **...** In order to **signcrypt** the message, Alice needs to do the following and keeps (z **...** The following outlines the weakness as regard group **signcryption**. **...**
Cited by 12 - Related articles - BL Direct - All 4 versions

A **signcryption** scheme based on integer factorization [PDF] from psu.edu
R Steinfeld... - Information Security, 2000 - Springer
... Tables 1 and 2 compare the efficiency of our scheme with the earlier **sign- cryption** scheme SCS1 **...** Then-Encryption (using Small Public Exponents and CRT decryption) and with ori- ginal **signcryption** scheme SCS1. **...** p−1 and q−1 are not smooth (ie have at least one large prime **...**
Cited by 58 - Related articles - BL Direct - All 12 versions

Provably secure encrypt-then-sign composition in hybrid **signcryption** [PDF] from psu.edu
IR Jeong, HY Jeong, HS Rhee... - Proceedings of the 5th ..., 2002 - portal.acm.org
... In the paper, we propose new encrypt-then-sign composition method in **sign- cryption** called DHEtS, and **...** To make a hybrid **signcryption** scheme, we can follow two different approach. One approach is to make a secure hybrid asymmetric encryption scheme which is made using **...**
Cited by 17 - Related articles - BL Direct - All 9 versions

[PDF] Shortened digital **signature**, **signcryption** and compact and unforgeable **key** agreement schemes [PDF] from psu.edu
Y Zheng - ... to IEEE P1363a: Standard Specifications for Public-Key ..., 1998 - Citeseer
... applications, it suffices to define KHk(m) = hash(k, m), where hash is a one-way hash **...** gxb mod p. Relevant public and **private** parameters are summarized in Table 2. The **signcryption** and unsigncryption **...** For Alice to **signcrypt** a message m to be sent to Bob, she carries out the **...**

Cited by 15 - Related articles - View as HTML - All 6 versions

Provably Secure Encrypt-then-Sign Composition in Hybrid **Signcryption**
I Rae Jeong, H Yun Jeong, H Sook Rhee... - ... Security and Cryptology ..., 2003 - Springer
... In the paper, we propose new encrypt-then-sign composition method in **sign- cryption** called DHEtS, and ... To make a hybrid **signcryption** scheme, we can follow two different approach. One approach is to make a secure hybrid asymmetric encryption scheme which is made using ...
Related articles

A survey of research on electronic auction
X CHEN... - Journal of China Institute of, 2002 - en.cnki.com.cn
... Xidian University, Xi抜n 710071, China). Electronic auction is one of the ... an,Shaanxi 710071,China);A Group **Signature** Scheme Based on Ring **Signature** Idea[J ... AN EFFICIENT ELECTRONIC AUCTION SCHEME BASED ON SECRET SHARING AND **SIGNCRYPTION**[J]; ...
Cited by 3 - Related articles - Cached - BL Direct

[PDF] Analysis and Design of Public **Key** Cryptographic Schemes — [PDF] from signcryption.org
R Steinfeld - 2003 - **signcryption**.org
... One such a problem is the integer factorization problem, which is also a very well known 'hard ... Definition of Security Models for General **Signcryption** Schemes. ... a range of precise security notions for both unforgeability and confidentiality of general **sign- cryption** schemes, which ...
Cited by 3 - Related articles - View as HTML - All 2 versions

[PDF] Yuliang Zheng The Peninsula School of Computing and Information Technology Monash University, McMahons Road, Frankston Melbourne, VIC 3199, ... — [PDF] from psu.edu
C **Signature**, EC **Signature**... - 1999 - Citeseer
... applications, it suffices to define KHk m = hash k; m , where hash is a one-way hash ... gxb mod p. Relevant public and **private** parameters are summarized in Table 3. The **signcryption** and unsigncryption ... For Alice to **signcrypt** a message m to be sent to Bob, she carries out the ...
Related articles - View as HTML - All 7 versions

Multipoint-to-multipoint secure-messaging with threshold-regulated authorisation and sabotage detection
A Goh... - ... and Multimedia Security. Advanced Techniques for ..., 2003 - Springer
... This is not demonstrated in TNR multi-sender sign- encryption—which simply uses one **key**-pair each for ... ZNR multi-**signcryption** with verified combination ... in any case required) of individually submitted s. This illustrates the efficacy of the ZNR **sign- cryption** approach which ...
Related articles - BL Direct - All 5 versions

[PDF] Using **Signcryption** to Build Compact and E cient Protocols for Unforgeable Session **Key** Establishment — [PDF] from psu.edu
Y Zheng... - 1999 - Citeseer
... 12 Page 13. Figure 3: Indirect Transport of **Key** Materials 6 **Signcryption** Based **Key** Establishment ... It would be pointed out that the digital **signature** scheme used by the CA in creating public **key** certi cates does not have to be one based on ElGamal **signature** scheme. ...
Related articles - View as HTML - All 3 versions

블록 암호 알고리즘을 사용하지 않는 인증
암호화 - 정보과학회논문지: 시스템 및 이론, 2002 - dbpia.co.kr
... **private key** - y B = g x B mod p : Bob's public **key** - hash : a one-way hash ... Scheme We describe the Bao-Deng **signcryption** scheme [9], which is based on Zheng's **signcryption** scheme [1 ... ciphertext c = E K2 (m) . - compute **commitment** r = hash (m ||K 1) . - compute **signature** s = k ...
Related articles

[PDF] Yuliang Zheng School of Computing and Information Technology Monash University Melbourne, VIC 3199, AUSTRALIA — [PDF] from psu.edu
H Imai - 1998 - Citeseer
... Figure 3: Indirect Transport of **Key** Materials 6 **Signcryption** Based **Key** Establishment ... It would be pointed out that the digital **signature** scheme used by the CA in creating public **key** certi cates does not have to be one based on ElGamal **signature** scheme. ...
Related articles - View as HTML - All 2 versions

[PDF] New E cient and Secure Protocols for Verifiable — [PDF] from psu.edu
D Catalano... - 1999 - Citeseer
... that a threshold **signature** scheme trivially gives a VS scheme when the **signature** sharer coincides ... relationship to fair public-**key** cryptosystems (FPKC) 34] in which one has to ... can be substituted with standard cryptographic techniques for privacy, **commitment** and authentication ...
Related articles - View as HTML - All 6 versions

[BOOK] Applied cryptography and network security: first international conference, ACNS 2003, Kunming, China, October 16-19, 2003: proceedings
J Zhou, M Yung... - 2003 - books.google.com
... Xiaoxi Han, Bo Zhu Digital **Signature** Proxy and Threshold One-Time Signatures ... Xie A Ring **Signature** Scheme Based on the Nyberg-Rueppel **Signature** Scheme ... 387 Sandeepan Chowdhury, Subhamoy Maitra Efficient Distributed **Signcryption** Scheme as Group **Signcryption**..... ...
Related articles - Library Search - All 4 versions

[PS] A Bibliography of Papers in Lecture Notes in Computer Science (2000) — [PS] from psu.edu
NHF Beebe - 2002 - Citeseer
... Comics [2463]. Commerce [793, 890, 1612, 2666, 2803, 321, 323, 2033, 322]. Commercial [2673]. Commercially [668]. Commit [143]. Commit/Isolation [143]. **Commitment** [719, 1571]. Commitments [1560]. Committal [2705]. Committed [729]. committing [1572]. ...

View as HTML - All 3 versions

[PS] A Bibliography of Papers in Lecture Notes in Computer Science (1997), Part 2 of 2 [PS] from psu.edu
NHF Beebe - vertex, 2002 - Citeseer
... Comment [2706]. Page 11. 11 Commerce [307, 1442, 1443, 1458, 1449, 1450, 2619, 2471, 1455, 2618, 1459, 2470, 2620, 1453]. **Commitment** [2681, 2775]. Commitments [1549]. Committees [2763, 1261]. Common [2021, 1978, 1374, 1806, 1552, 682]. Common-Pool [1978]. **...**
Related articles - View as HTML - All 4 versions

[PS] A Bibliography of Papers in Lecture Notes in Computer [PS] from psu.edu
NHF Beebe - way, 1999 - Citeseer
... Commands [1554]. Commerce [39, 919]. **Commitment** [391]. Communicating [785, 552]. **...** Conditioning [576]. Conditions [614, 2067, 134]. Conference [47, 1524]. Conference-**Key** [47]. Con guration [874, 870, 865, 872, 909, 232, 954, 871, 1884]. Con guration-Based [232]. **...**
Related articles - View as HTML - All 2 versions

Create email alert

signcryption IBE signature commitm Search

Go to Google Home - About Google - About Google Scholar